Hakin9

Vol.4 No.1
Issue 01/2014(11) ISSN: 1733-7186

starterkit

TEASER

HACKING SOCIAL MEDIA

15 STEPS TO HACKING WINDOWS

PROTECTING YOUR FACEBOOK ACCOUNT

OBTAINING CLASSIFIED INFORMATION

SYN FLOOD ATTACK SCENARIO

ANTI-THREATS STRATEGIES

PLUS

RIGHTS OF A CLOUD CUSTOMER BEING

Dr.Web 9.0

for Windows — the rapid response anti-virus

1. Reliable protection against the threats of tomorrow
2. Reliable protection against data loss
3. Secure communication, data transfer and Internet search

www.drweb.com

Free 30-day trial: https://download.drweb.com

New features in Dr.Web 9.0 for Windows: http://products.drweb.com/9

FREE bonus — Dr.Web Mobile Security:
https://download.drweb.com/android

Developing for Amazon Web Services?

Attend Cloud DevCon!

Cloud DevCon

June 23-25, 2014
San Francisco
Hyatt Regency Burlingame

www.CloudDevCon.net

Attend Cloud DevCon to get practical training in AWS technologies

- Develop and deploy applications to Amazon's cloud
- Master AWS services such as Management Console, Elastic Beanstalk, OpsWorks, CloudFormation and more!
- Learn how to integrate technologies and languages to leverage the cost savings of cloud computing with the systems you already have
- Take your AWS knowledge to the next level – choose from **more than 55 tutorials and classes,** and put together your own custom program!
- Improve your own skills and your marketability as an AWS expert
- Discover HOW to better leverage AWS to help your organization today

Register Early and SAVE!

A BZ Media Event

CloudDevCon

HACKING SOCIAL MEDIA

Table of Contents

Dear Readers,

I have a pleasure to deliver next issue to you. While working on this issue, we had a simple goal in our minds. We wanted to provide you with an issue that be helpful for you. Our aim is to make each Reader benefit from our Magazine, gain valuable knowledge and practical skills.

Also, some of you know that we have launched our blog. On our blog you can find plenty of free articles! If you still have not been there, please go to: http://blog.hakin9.org/.

Also, on our website you can find brand new forum where you can interact with other Readers. Have you been there? No? You can simply go here: https://hakin9.org/forum/.

What is important for us is that you are a part of our community. We give a chance to every Reader who would like to share his knowledge. If you have any interesting issue to discuss, we are here for you!
We are a company with mission. Every day we are here for you, ready to change the world and make it more comprehensive for you!

Remember that you can always write to us at en@hakin9.org or directly to me at ewa.duranc@hakin9.org. Join our forum, meet other hackers, feel free to enter our community and stay with us forever!

Thank you for being with us!

Ewa Duranc,

Product Manager.

Editor in Chief: Ewa Duranc
ewa.duranc@hakin9.org

Betatesters & Proofreaders: Aidan C., Phil Patrick, Elia Pinto, Kishore PV, Hani Ragab

Special thanks to our Beta testers and Proofreaders who helped us with this issue. Our magazine would not exist without your assistance and expertise.

Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@hakin9.org

Product Manager: Ewa Duranc
ewa.duranc@hakin9.org

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

Art. Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@hakin9.org
DTP: Ireneusz Pogroszewski

Marketing Director: Ewa Duranc
ewa.duranc@hakin9.org

Publisher: Hakin9 Media sp. z o.o. SK
02-676 Warszawa, ul. Postępu 17D
NIP 95123253396
www.hakin9.org/en

15 Steps to Hacking Windows Using Social Engineering Toolkit and Backtrack 5

by Matias R. Iacobuzio

This article aims to demonstrate fundamental Social Engineering principles and to present Social Engieneering Attacks techniques, such as Site Cloner. Social Engineering Toolkit are presented and the final phase is to analyze their results.

> ***"The Social-Engineer Toolkit (SET) is specifically designed to perform advanced attacks against the human element. SET was designed to be released with the http://www.social-engineer.org launch and has quickly became a standard tool in a penetration testers arsenal. SET was written by David Kennedy (ReL1K) and with a lot of help from the community it has incorporated attacks never before seen in an exploitation toolset. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test".***

Actually this hacking method will works perfectly with DNS spoofing or Man in the Middle Attack method. Here in this tutorial I'm only write how-to and step-by-step to perform the basic attack, but for the rest you can modified it with your own imagination.

In this tutorial we will see how this attack methods can owned your computer in just a few steps…

For your information: The success possibility of this attack depend on victim browser. If the victim never update their browser, the possibility can be 85% or more.

Hacking Windows Using Social Engineering Toolkit and Backtrack 5 in 15 steps:

Step 1

Change your work directory into `/pentest/exploits/set/`

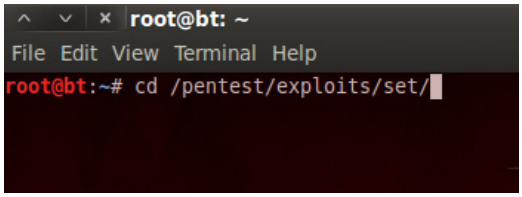

Figure 1. First step

Srep 2

Open Social Engineering Toolkit (SET) `./set` and then choose "Website Attack Vectors". We will attack victim via internet browser, also in this attack we will attack via website generated by Social Engineering Toolkit to open by victim, so choose "Website Attack Vectors" for this options.

Figure 2. Website Attack Vectors

Step 3

Usually when users are opening a website, they don't think that they are opening suspicious website that including malicious script to harm their computer. In this option we will choose "The Metasploit Browser Exploit Method" because we will attack via victim browser.

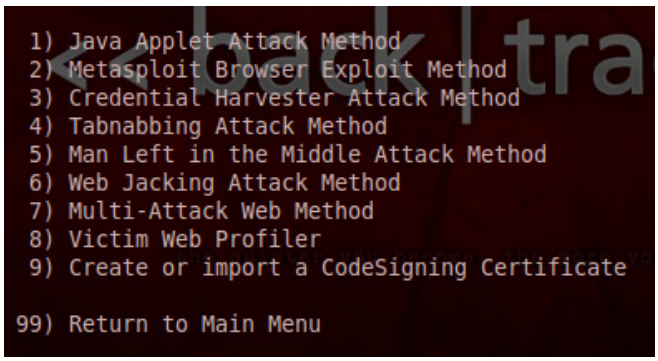

Figure 3. Metasploit Browser Exploit Method – here at point 2

Step 4

The next step just choose “Web Templates”, because we will use the most famous website around the world that already provided by this Social Engineering Toolkit tools.

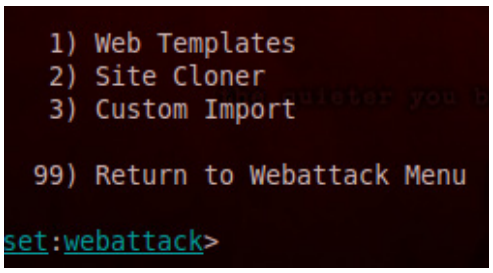

Figure 4. Web Templates at panel

Step 5

There are 4 website templates Ready To Use for this attack methods, such as GMail, Google, Facebook, and Twitter. In this tutorial I will use Google, but if you think Facebook or Twitter are better because it’s the most accessed website, just change into what do you want.

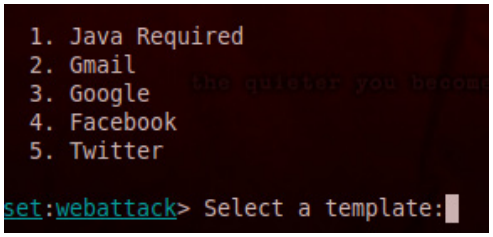

Figure 5. Choosing a website

Step 6

For the next step… because we didn’t know kind of vulnerability that successfully attack the victim and what type of browser etc, in this option we just choose “Metasploit Browser Autopwn” to load all vulnerabilities Social Engineering Toolkit knows. This tools will launch all exploit in Social Engineering Toolkit database.

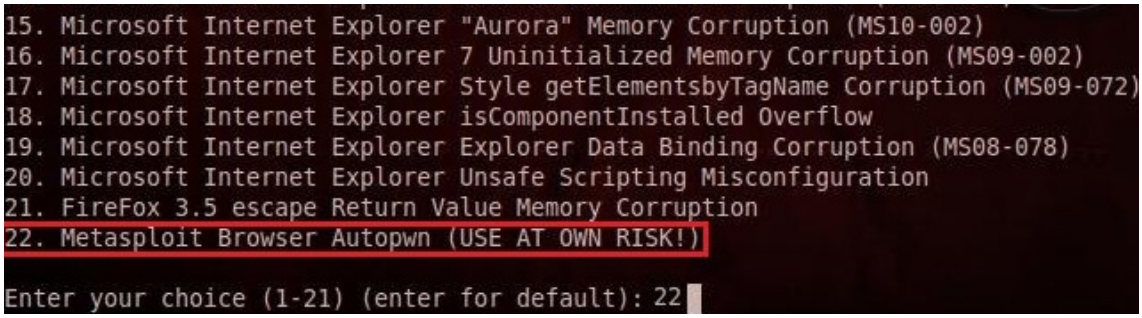

Figure 6. Choosing Metasploit Browser Autopwn

Step 7

For payload options selection I prefer the most using Windows Shell Reverse_TCP, but you also can choose the other payload which is most comfortable for you.

Figure 7. Choosing the payload

Step 8

The next step is set up the Connect back port to attacker computer. In this example I use port 4444, but you can change to 1234, 4321, etc.

Figure 8. Typing the connect port

Step 9

The next step is... just wait until process are completed and the server is running.

Figure 9. Processing

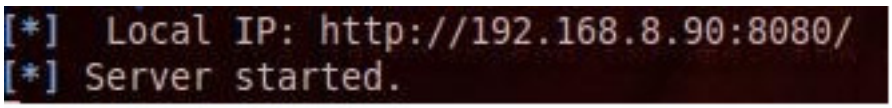

Figure 10. Information about start of server

Step 10

When the link given to user, the victim will see looks-a-like Google (fake website). When the page loads it also load all malicious script to attack victim computer.

Figure 11. Fake website (see the details of web address)

Step 11

In attacker's computer, if there's any vulnerability in victim computer browser, will return sessions value, which means the exploit successfully attacked victim's computer. In this case the exploit create new fake process named "Notepad.exe".

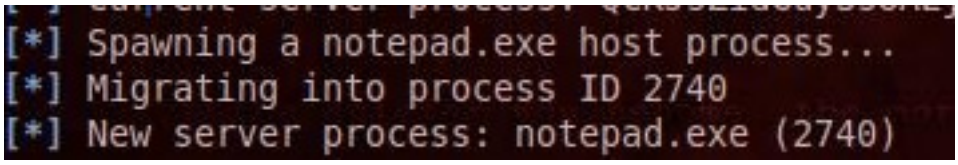

Figure 12. Confirmation of successfull attack

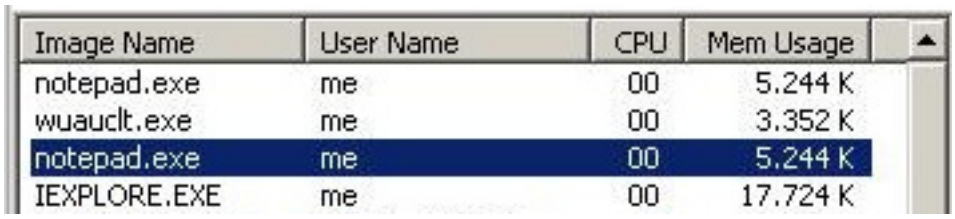

Figure 13. New fake process in victim's system

Step 12

To view active sessions which is already open by the exploit, type "sessions -l" for listing an active sessions. Take a look to the ID…we will use that ID to connect to victim computer.

Figure 14. ID of victims

Step 13

To interract and connect to victim's computer use command "sessions -i ID". ID is numerical value that given when you do sessions -l. You can see the example in picture below.

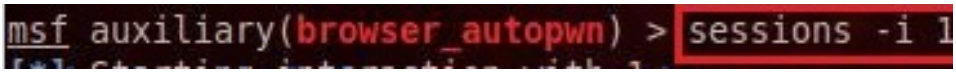

Figure 15. Typing the command 'sessions -i ID'

Step 14

Victim computer is already owned!

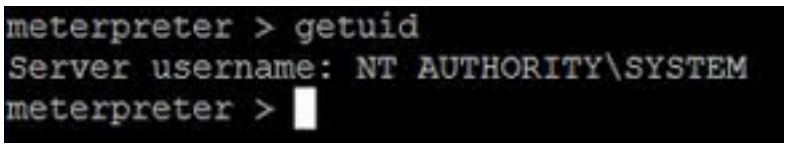

Figure 16. Take over the victim's system

To create this tutorial I used Virtual Machine, so it will not harm other computer and also you can do a lot of experience with your OS.

About the Author

Matias R. Iacobuzio – Professional with 8+ year of experience in the field of IT Security, Threat and vulnerabilities Analist in Cargill and Proficient in IT security awareness programs, Network based forensics, Exploit Development, penetration testing and wireless penetration testing. Proven track record in IT security training and trained over 1,000+ students and over 1000+ professionals in the regions of Latin America and USA. Certified: ITIL v3, COBIT v5, ISO27001 and CEH, coming son CISM.
View my profile on LinkedIn
E-mail: kalq85@gmail.com

Threats and Anti-threats Strategies for Social Networking Websites

by Amir Roknifard

Social networking websites are not only to communicate or interact with other people globally, but also one effective way for business promotion. Relevance of the study due to the fact that with increased number of users of social networks, the number of attacks carried out by hackers to steal personal information and use of your user account in order to send unauthorized messages called spam is also raised. To address these security issues, network and security managers often turn to network policy management services such as firewall, Intrusion Prevention System (IPS), antivirus, and Data Loss Prevention systems (DLP).

What we will learn:

In this paper, we study the cyber threats in social websites, classify their types, discuss the cyber threats and suggest the anti-threats strategies and visualize the future trends of such hoppy popular websites.

Online Social Networks (OSN) such as Facebook, Tweeter, MySpace etc. play an important role in our society, which is heavily influenced by the Information Technology (IT). In spite of their user friendly and free of cost services, many people still remain reluctant to use such networking sites because of privacy concerns. Many people claim, these sites have made the world more public and less private – consequently a world with less morale is evolving. Some consider this social change as positive because people are more connected to each other. Nowadays, millions of internet users regularly visit thousands of social website to keep linking with their friends, share their thoughts, photos, videos and discuss even about their daily-life. Social networks can be traced back to the first email which was sent in 1971 where two computers were sitting right next to each other. In 1987 Bulletin Board System exchanged data over phone lines with other users and lately in the same year the first copies of early web browsers were distributed through Usenet. Geocities was the first social website founded in 1994. Theglobe.com launched in 1995 and gave people the ability of interacting with others, personalize and publish their files on the Internet. In 1997, the America on Line (AOL) Instant Messenger was lunched. In 2002, Friendster was lunched and within three months more than 3 million users were using it. In 2003, MySpace was lunched and in the following years many other social networking sites were lunched such as Face book in 2004, Twitter in 2006 etc [1]. There are so many social networking sites and social media sites that there is even search engine for them [2]. Further, there are specialized websites which allow users to create their social networking sites such as Ning and KickAppls [3]. These social websites have had positive and negative impacts; so many people waste most of their time on using these websites, which results in losing their jobs or colleges or even their natural social lives and families! Many others post copyrighted materials without authorizations, or pornographic or illegal contents. Some of the users, smart-users, use social networking websites in a very positive way; as happen now in the Spring of Arab World!

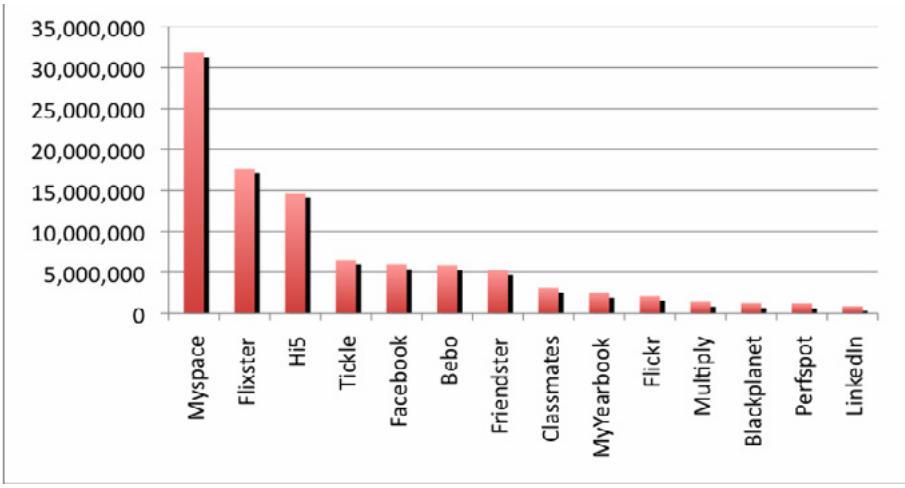

Figure 1. Total number of social networks users (Rapleaf's data)

The Internet today, unfortunately, offers to the cybercriminals many chances to hack accounts on social network sites and the number of malicious programs that target the social web sites is very huge. (Ref: Figure 2).

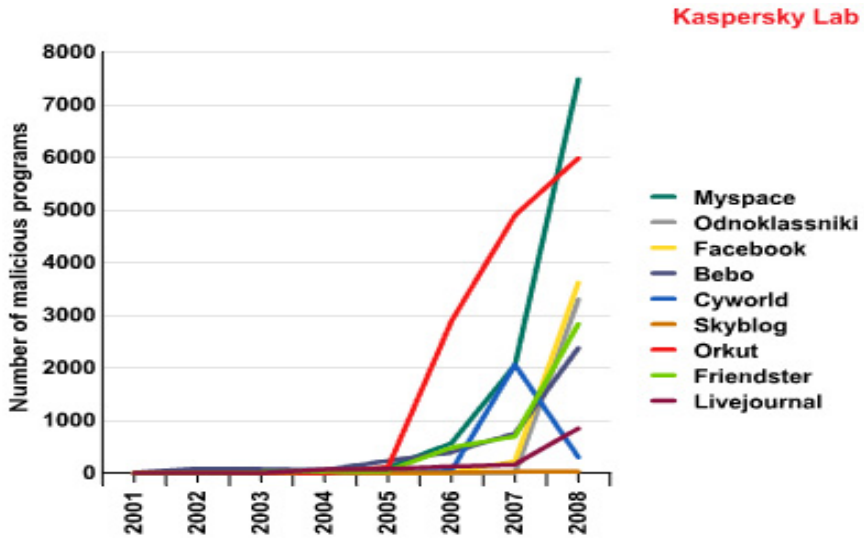

Figure 2. Number of malicious programs targeting popular social networking sites

The rest of the paper is organized as follows. Section 2 discusses the security policy background. In Section 3, we present the categorized types of social networks. In Section 4, we discuss and analysis the cyber threats in social websites. In Section 5, it has been recommended the anti-threats strategies. In Section 6, the future trends of social networks have been analyzed. In Section 7, we reveal the risks prevention and threats vulnerabilities. Finally, we ended our paper with the conclusion at Section 8.

Security Policy Background

In spite of an organization's size, their businesses, or the extent to which it uses technology, information security is an important matter that should be addressed by explicit policies. However, the settlement of security policies is itself based on a specific framework that requires methodology to write, structure, effective review, approval, enforcement and awareness process [6]. Although this paper doesn't have the goal to stress the topic security policies, the most important factor to be considered to develop the proposed framework is having an established security policy. Security policies are high-level statements that provide guidance to those who must make present and future decisions. An information security policy document is vital for many reasons. Beyond the definition of roles and responsibilities for workers, partners, suppliers, a policy document sensitizes them to the potential threats, vulnerabilities and problems associated with modern information systems.

A consistent awareness program is fundamental to achieve the security policy goals. Education and training helps minimize the cost of security incidents, and helps assure the consistent implementation of controls across an organization's information systems. Currently the effectiveness of security policies considering data leakage is an important concern. Regardless of the type or mode of data leakage, recent research [9] reveals that one out of four companies does not even have a security policy and for businesses with policies, the findings reveal a significant gap between the beliefs of security staff regarding employee compliance and the actual behavior of them. The reasons why employees knowingly overlook or bypass security policies and put corporate data at risk are mainly a result of a failure to communicate the security policies and create an awareness behavior. The proposed framework presents an adaptive strategy to the awareness program. A security policy detailing information classification is essential to sustain a framework to avoid data leakage. This policy will create the basis of ownership responsibilities for files, databases and other shared information, indicating who have been granted authority to originate, classify, modify, or delete specific information. The policy should also indicate the transportation mode, third-party interactions, labelling, life cycle, declassification, and information destruction. Depending on the information type and its criticality to the owner, the information may be assigned, for example as public, secret, confidential or internal use only.

Taxonomy Of Social Networks

Generally, a social network is a social structure made up of individuals or organizations, which are connected, by one or more specific types of interdependency, such as friendship, common interest, and exchange of finance, relationships of beliefs, knowledge or prestige. Social networks can also be defined as those websites that enable people to form online communications and exchange all types of data. It includes the following.

First, Social networking sites such as MySpace, Face book, Windows Live Spaces, Habbo, etc. and the second Social media sites such as You tube, Flicker, Digg ,Metacafe, etc. Table 1 illustrates the social websites according to continent and regions.

Table 1. Social websites according to Continent and Region

Continent/region	Dominant social websites
Africa	Hi5, Facebook
America (North)	MySpace, Facebook, Youtube, Flicker, Netlog
America (Central &South)	Orkut, Hi5, Facebook
Asia	Friendster, Orkut, Xianonei, Xing, Hi5, Youtube, Mixi
Europe	Badoo, Bedo, Hi5, Facebook, Xing, Skyrock, Ployaheod, Odnoklassniki.ru.V Kontakte
Middle East	Facebook
Pacific Island	Bedo

In Table 2, the top five popularity trafficked social media sites:

Table 2. Top five popularity trafficked social media sites

Site Name	Primary Shared Media
YouTube	Videos
Flicker	Images
Digg	Book marks
Metacafe	Videos
Stumbleupon	Cool Contents

Moreover, Youtube is the third most visited Web Site after Yahoo and Google but flicker is the 39th most visited web site [5].

Cyber Threats In Social Networking Websites

Lately, social networks attract thousands of users who represent potential victims to attackers from the following types (Ref: Figure 3) [6, 7]. Phishing is a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party. Phishing attacks today typically employ generalized “lures”. For instance, a hacker misrepresenting himself as a large banking corporation or popular on-line auction site will have a reasonable yield, despite knowing little to nothing about the recipient. Phishing attacks can incorporate greater elements of context to become more effective. In other forms of context aware phishing, an attacker would gain the trust of victims by obtaining information about their bidding history or shopping preferences. Phishing attacks can be honed by means of publicly available personal information from social networks [9]. First hackers and spammers who use social networks for sending fraudulent messages to victims “friend”, Cybercriminals and fraudsters who use the social networks for capturing users data then carrying out their social-engineering attacks

and Terrorist groups and sexual predators who create online communities for spreading their thoughts, propaganda, views and conducting recruitment.

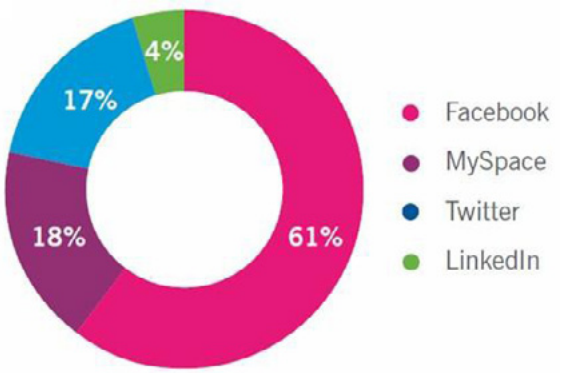

Figure 4. Threats percentage-pose on social networks (Sophos 2010 Security Threat Report) Cyber threats that might the users face can be categorized into two categories.

Privacy Related Threats

Privacy concerns demand that user profiles never publish and distribute information over the web. Variety of information on personal home pages may contain very sensitive data such as birth dates home addresses, and personal mobile numbers and so on. This information can be used by hackers who use social engineering techniques to get benefits of such sensitive information and steal money.

Traditional Networks Threats

Generally, there are two types of security issues: One is the security of people. Another is the security of the computers people use and data they store in their systems. Since social networks have enormous numbers of users and store enormous amount of data, they are natural targets spammers, phishing and malicious attacks. Moreover, online social attacks include identity theft, defamation, stalking, injures to personal dignity and cyber bulling. Hackers create false profiles and mimic personalities or brands, or to slander a known individual within a network of friends.

Anti Threats Strategies

Recent work in programming language techniques demonstrates that it is possible to build online services that guarantee conformance with strict privacy policies. On the other hand, since service providers need private data to generate revenue, they have a motivation to do the opposite. Therefore, the research question to be addressed is to what extent a user can ensure his/her privacy while benefiting from existing online services. A novel approach, called NOYB (None Of Your Business), was discussed in [7], which provides privacy while preserving functionalities provided by service providers. Users willingly share personal identifying information, but do not have a clear idea of who accesses their private information or what portion of it really needs to be accessed. OSNs can be examined from a viewpoint of characterizing potential privacy leakage [10]. That is, we can identify what bits of information are currently being shared, how widely they are available, and what users can do to prevent such sharing. The third-party sites that track OSN users play a major role in these kinds of attacks causing privacy leakage on popular traditional websites. In the long run, we can identify the narrow set of private information that users really need to share to accomplish specific interactions on OSNs so that privacy can be enhanced further. Privacy can also be preserved by restricting the ability to recover the real data from the fake data to authorized users only.

In this section we present the different types of cyber threats in social networks and found the most of threats happens due to the factors which are listed as below:

- Most of the users are not concern with the importance of the personal information disclosure and thus they are under the risk of over disclosure and privacy invasions,
- Users, who are aware of the threats, unfortunately choose inappropriate privacy setting and manage privacy preference properly,
- The policy and legislation are not equipped enough to deal with all types of social networks threats which are increase day by day with more challenges, modern and sophisticated technologies,
- Lack of tools and appropriate authentication mechanism to handle and deal with different security and privacy issues,

Because of the above mentioned factors that cause threats, we recommended the following strategies for circumventing threats associated with social website:

- Building awareness the information disclosure: users most take care and very conscious regarding the revealing of their personal information in profiles in social websites,
- Encouraging awareness -raising and educational campaigns: governments have to provide and offer educational classes about awareness -raising and security issues,
- Modifying the existing legislation: existing legislation needs to be modified related to the new technology and new frauds and attacks,
- Empowering the authentication: access control and authentication must be very strong so that cybercrimes done by hackers, spammers and other cybercriminals could be reduced as much as possible,
- Using the most powerful antivirus tools: users must use the most powerful antivirus tools with regular updates and must keep the appropriate default setting, so that the antivirus tools could work more effectively,
- Providing suitable security tools: here, we give recommendation to the security software providers and is that: they have to offers some special tools for users that enable them to remove their accounts and to manage and control the different privacy and security issues.

Future Trends Of Social Networking Websites

In spite of the development and advanced technologies in social networking websites adjustment, a few are listed as below:

- A need for more improvements for social networks so that they can allow users to manage their profiles and connecting tools,
- A need for convergence and integration of social networks and future virtual worlds,
- Needs for data integration from different networks, i.e. identification of all contents related to specific topic. This needs particular standards and sophisticated technology supported by social networks providers,
- Many social networks need standard application programming interfaces, so that users can import and export their profiling information by using standard tools. (For example, Facebook and Google have applied new technologies that allow user data portability among social websites, representing a new source of competition among social networking service),

We hope that in the near future, one can by single sign-in functionality use over websites, that is, the user IDs are portable to other websites.

Moreover, virtual worlds have distinct virtual economies and currency that based on the exchange of virtual goods. Games are one of the newest and most popular online application types on social websites. Here, we have to mention the importance of privacy and security to save users from fraudsters who attempt to steal social networking credentials and online money.

Finally, we have to mention that the advances in the social websites and mobile-phone usage will effect on the growing of using mobile social networking by adding more features and application not only to mobiles, but also to social televisions for future chat, email, forums, and video conferencing [8, 9].

Risks Prevention And Threats Vulnerabilities

In this Section, we supply with some important recommendations to help social network users stay save by applying the followings:

- Always have very strong passwords on your emails and other social web sites,
- Limiting the provided personal information in the social web sites as much as you can,
- Change your passwords regularly, so that your information can be out of reach by hackers,
- Provide with the minimum amount of information to the website and internet due to the publicity of the internet,
- Don’t trust online others and don’t answer on special questions from unknown users or companies i.e. be skeptical,
- Check privacy policies and be aware of unknown emails and links provides by unknown users,

To prevent detecting emails address by spammer techniques, write the email: xyz@hotmail.com as xyz at hotmail dot com.

Summary

Although social networking websites offer advanced technology of interaction and communication, they also raise new challenges regarding privacy and security issues. In this paper, we briefly described the social networking web sites, summarized their taxonomy, and highlighted the crucial privacy and security issues giving some essential anti-threats strategies with the perspective of the future of the social networking websites.

We think that the advancement of new technology in general and social websites in particular will bring new security risks that may present opportunities for malicious actors, key loggers, Trojan horses, phishing, spies, viruses and attackers. Information security professionals, government officials and other intelligence agencies must develop new tools that prevent and adapt to the future potential risks and threats. It can also safely manipulate the huge amount of information in the internet and in the social websites as well.

References

[1] *http://www.onlineschools.org/blog/history-of-social-networking/*
[2] Social networking sites searchengine, *http://findasocialnetwork. com/search.phpS*
[3] B. Stone, Is Facebook growing up too fast, The New York Times, March 29, 2009
[4] “Using Facebook to Social Engineer Your Way Around Security”, http://www.eweek.com/c/a/Security/Social-Engineering-Your-Way-Around-Security-With-Facebook- 277803/ 05.20.2010
[5] *www.securelist.com*, ”Instant” threats, Denis Maslennikov, Boris Yampolskiy, 27.05.2008.
[6] Won Kim , Ok-Ran Jeong, Sang-Won Lee , “On Social Websites” , Information Systems 35 (2010), 215-236.
[7] Kaven William, Andrew Boyd, Scott Densten, Ron Chin, Diana Diamond, Chris Morgenthaler, “ Social Networking Privacy Behaviors and Risks” ,Seidenberg School of CSIS, Pace University, White Plains, NY 10606, USA.
[8] Abdullah Al Hasib, “Threats of Online Social Networks”, IJCSNS, Vol. 9, No 11, November 2009.
[9] Anchises M. G. de Paula, “Security Aspects and Future Trends of Social Networks”, IJoFCS (2010) , 1, 60-79.

[10] D. Boyd, N. Ellison, Social network sites: definition, history, and scholarship, Journal of Computer- Mediated Communication 13 (1) (2007) article 11.
[11] Gilberto Tadayoshi Hashimoto, Pedro Frosi Rosa, Edmo Lopes Filho, Jayme Tadeu Machado, A Security Framework to Protect Against Social Networks Services Threats, 2010 Fifth International Conference on Systems and Networks Communications.
[12] "Data Loss Prevention Best Practices", *http://www.ironport.com/pdf/ironport_dlp_booklet.pdf* 05.20.2010.
[13] "The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained", *http://us.trendmicro.com/imperia/md/content/us/trendwatch/researcha* and analysis/the_real_face_of_koobface_jul2009.pdf 05.19.2010.

About the Author

Amir Roknifard (MCSE, CCNP, CISSP, ISO27002) is an information security expert with more than nine years of experience in IT and Security. He was not only involved in general security projects, but also served as a project manager for some unique projects like the penetration test of the Central Bank of Iran. His experience includes work in cooperation with a team of experts who developed the CSIRT in Iran; He developed an idea of the network of sensors with a centralized analyzer piping to the CSIRT R&D department. His fields of interest are access control and cryptography.

VoIP and Cloud: Security Issues

by Mirko Raimondi

In today's economy, companies are looking for at cost saving measures and Clouding provides much greater flexibility than older computing models. There are a lot of benefits using Clouding architectures: the main benefit is about the cost-effective, since you pay as you go. Another benefit is the portability: an user can work from workspace, home, or at customer locations; this increases in mobility means that the employees could access to the informations from anywhere.

Even if it is not widely adopted yet, VoIP cloud services open new opportunities to telecom business. When a small company wants to begin a business in VoIP telecommunications, if it choose to the traditional model, it will have to buy server equipment and to build all network infrastructure. Instead of buying and maintaining a traditional VoIP infrastructure, one could decide the alternative of Clouding where equipments are subscribed and not bought; in this case there are no expenses to pay in advance. Thus, today's VoIP business can be started and run without making large initial investments. Furthermore, there's another reason to choose Cloud services instead of traditional models: more frequent server software updates, getting the benefit to free-up employees which can have been occupied performing updates, installing patches and providing application support. Finally, Clouding is a great contribution to the energy saving, since with more servers shared by carriers less electricity is spent and existing equipment gets to be used more efficiently.

There are important security threats that need to be evaluated when considering moving VoIP applications with sensitive data to public and shared Cloud environments. Hence, Cloud providers must develop sufficient controls to provide the same level of security than the organizations would have if the Cloud were not used. The main reason which VoIP cloud services are not widespread is that client carriers are unsure whether hosting service providers can provide a reliable service with the necessary data security level. But unfortunately, few people have really understood that data security is also not guaranteed when sevices operate on the equipment owned by carriers.

Cloud Features

Clouding has the characteristics reported in the following.

- Resource Pooling: resources of the provider are pooled and shared between many users;
- Rapid Elasticity: in few of minutes resources could be provisioned to scale out and released to scale in;
- Network Access: resources are accessible through standard network protocols over the Internet;
- On-demand self-service: resources can be provisioned via automated systems;
- Measured Service: providers measure CPU charges, network bandwidth, memory and other resources.

Every type of Cloud service has the capabilities before reported but the various service models differ in both form and function. There are three fundamental Cloud types which describe and define the service contents. They're reported in the detailed list reported below.

- Infrastructure as a Service (IaaS): you are buying an infrastructure and users can access to the network, devices, Storage Area Network (SAN) and other resources through the provider; it also use every kind of software including Operating System (OS) and applications. Users are not in charge of the cloud infrastructure, they only have authority on OS, SAN, distributed software and network components which are going to be used. This model is similar to a utility company model, where you pay for what you use. The user has access in a form that is close to an on-demand service to an arbitrary number of network-connected servers. An arbitrary number of servers are multiplexed onto a fixed number of physical devices machines (Host), generally using Virtual Machines (VMs) running on Hypervisors. Hypervisor,

also said Virtual Machine Monitor (VMM), is a piece of computer software, firmware or hardware which creates and runs VMs. A computer whereon an Hypervisor is running one or more VMs is defined as a Host Machines and each VM is called Guest Machine;

- Platform as a Service (PaaS): provider provides a platform for your use. Users can develop and run software over cloud computing infrastructure via programming languages, libraries, services and all the tools supported by the provider. Services provided include all phases of the System Development Life Cycle and can use Application Program Interfaces, website portals, or gateway software. Users are not in charge of the network, servers, OS and SAN belonging to the Cloud infrastructure, they can just change few configuration settings;

Software as a Service (SaaS): platform and software utilities are supported and provided by the provider. Users can access to applications via different devices as thin clients and network browsers.

Cloud Open Threats

A Cloud infrastructure is substantially subject to the same security threats that has a standard network infrastructure. In this article the author will try to focus just on security threats where cloud-based systems are different from traditional networks.

In the following, the author will assume that VoIP systems are runnig within VMs running on Hypervisors with local storage and access to SAN as shown in Figure 1. The victim is assumed to have one or more VMs in the cloud.

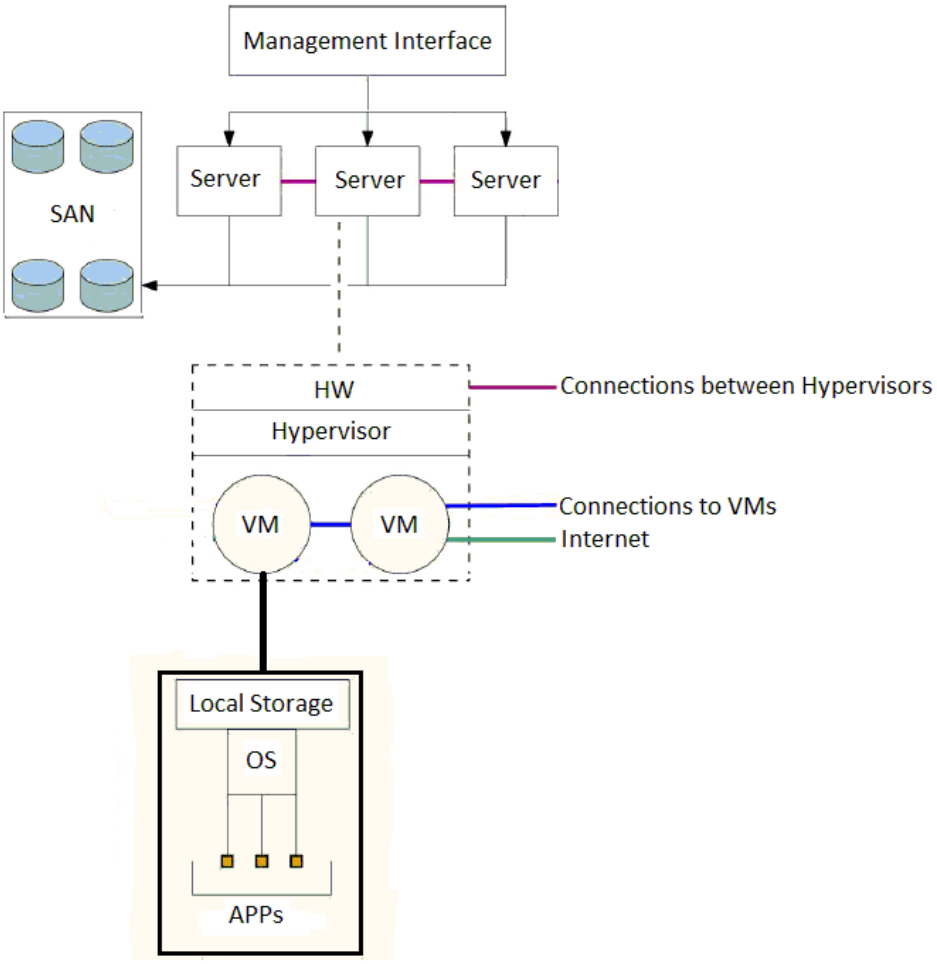

Figure 1. IaaS Platform

The author will also assume that the attacker is either on the public Internet connecting to the victim VM or that the attacker has a VM with the same Cloud service as the victim VM. For some attack the author will assume that the attacker has a VM on the same Host (running on the same Hypervisor) as the target. Finally, in every scenario the software (Apps and OS) of the victim is believed as secure, in this way the attacker could just to take advantage of the fact that the victim is using a Cloud infrastructure.

- Denial of Service (DoS): in a Cloud infrastructure CPU, RAM, disk and network resources are shared between users. If an attacker consumes a large amount of resources, all users will get a decrease in performance generating a DoS attack. As countermeasure, user applications could be migrated to other part of the Cloud infrastructure with less resource contention but keeping in mind that resources are not unlimited. Cloud providers have employed several strategies in order to realize a partition of the resources in such a way, hence DoS become less likely. Some provider has divided the Cloud in zones which are designed in order to fail independently. To maximize the uptime, the applications must be replied in multiple zones allowing fail-over among them. Within data centers, networks are partitioned by routers and network-level Quality of Service (QoS) mechanisms. Some Hypervisor implements CPU schedulers which give just a fixed par of CPU and network bandwidth belonging to the Host, but this strategies is weak since attackers could manipulate the Hypervisor scheduler stealing network resources and CPU. Moreover, even when user's VM gets its allocated share of resources, it may not get them in a timely fashion implying increases in network response latency and this increases in latency can be particularly annoying in Real-Time applications such as VoIP;

- Infrastructure Compromise: this kind of attacks are yet rather unexplored, the attacker gets a privileged level obtaining root access on the machine. In order to realize the attack, either the management interface of the provider or the cloud infrastructure is exploited by the attacker. Some Cloud service provides a Simple Object Access Protocol (SOAP) defined by an XML schema, in this way an attacker could send a SOAP message with XML signatures and the attacker just needs a valid signed SOAP message. SOAP messages can be easy to get, for example, providers used to including them in public message posted in order to aid debugging. The attacker could use these messages and their keys to forge a new malicious message, with this forged message the attacker can cheat the Host into thinking that the he is a legitimate administrative user for that domain, in this way the attacker obtains the complete control;

- Data Confidentiality: users want that Cloud providers both store and serve their data, but sometimes they do not want that cloud providers to have free access to their data. Currently, there are not any default ways adopted in order to prevent cloud providers from having free and ready access to the data they are storing and serving. Malicious providers of Cloud services could even freely abuse the data they are given access since all data is stored in the clear. One solution that could be taken is to encrypt data resident in the Cloud, but a simple encryption won't so straightforward to implement since the cloud-based VMs are used to process cloud-resident data, hence if the data is encrypted the Cloud provider also has the data keys;

- Data Availability and Integrity: Cloud providers guarantee uptime in their service but they do not guarantee availability or data integrity. Cloud providers have not the commitment to prevent or notify to the users data corruption or loss of data availability. Users just can verify data accessibility and integrity by manually accessing all remotely stored information. The goal for the next years is to make customer checks of data more feasible;

- Breaches of Confidentiality: information about data stored inside VMs could be damaged through resource contention with a co-located attacker VM. For example, attackers would start up several instances (even over 100 in order to gain the desired results) with the aim to hit the victim. Once the attacker has chosen the victim, he tries to influence the victim to react in a way that they could predict and in this way the attacker can extract informations. This attack exploits the fact that many VMs will run on the same Host. The creation of many instances is done in order to make it feasible for the attacker to get an access into the victim Host. Attackers can use multiple ways to determine if they had got an access on the same Host of the victim. The mainly used is a network-based strategy which uses a simple IP scans in order to determine if the attacker and the victim share the same administrative IP address (the IP address of their instance). Another is to check whether there is a low latency network path with the target (whether packets can be exchanged with minimal transmission delay). Moreover, the attacker could control whether accesses to the victim increase the rate of cache misses in his own VM, in this case the attacker and the victim are sharing the same hardware. Whether the attacker shares an Host with the victim, timing and cache interference effects between VMs could be used to get information from the target, such as

OS and cryptographic keys. One countermeasure could be to prevent the users from sharing hardware guaranteeing exclusive access to the Hosts. Providers may also randomize the assignment of VMs, in order to reduce the probability of co-location between attacker and victim. Furthermore providers must to minimize potential communication channels between VMs. Another approach that a cloud provider could take is to guarantee exclusive access to CPU caches through cache partitioning. In partitioning the cache, the amount of cache information overflow that may cause information leakage is reduced and the attacker can't monitor what is being altered within the cache by other VMs.

Security About Unified Communications (UC)

UC is the integration of Real-Time communication services such as IP telephony, video conferencing, instant messaging (chat), presence information, call control, speech recognition and data sharing with non Real-Time communication services such as unified messaging (integrated voicemail, e-mail, SMS and fax). UC is not necessarily a single product, but could be a pool of products that provides a consistent unified user-interface and user-experience across multiple devices and media-types.

As already reported, VoIP Cloud operators and hosted service providers offer several new benefits: improved cost performance, ease of management, investment protection and enhanced UC services. Cloud service operators hold an increased concentration of user service information and resources within their operations which imply added security risk.

UC is the mainly component which grants business of all sizes access to scalable and flexible communications services and applications. Service and reliability are the two key components of business grade UC delivery. Users expect Cloud operators to provide availability and security, as was found in premises based PBX, voice mail, and network services. While cloud operators can to deliver flexible and scalable service solutions, customers relinquish much of the control of the system to the operator. UC is based on a collection of open standards and technologies based on IP networking and data infrastructure. Delivering Cloud-based services entail that the provider must consider the security impact of managing valuable and sensitive user communications. Cloud service providers have adopted specialized security solutions to protect databases, e-mails and web services. Hosting UC services present Cloud operators with a significant new set of risks.

- If a communication port is opened, even for a few seconds, the system is exposed to a DoS;
- Weak authentication for an endpoint can be exploited for toll fraud: billing and call management systems can be exploited, in this way the attacker steal expensive international calling services;
- Protocol injection in media or signaling streams can be used by attackers in order to eavesdrop on calls and to access confidential information.

UC Cloud operators must implement security policies that encompass other threats like: access control, anti-virus and disaster recovery planning. These policies must be coupled with authentication schemes, password protections, and encryption requirements.

Intrusion Detection Systems (IDSs)

IDSs are one of the practical coutermeasure that could be used in order to avoid the attacks reported in previous sections. IDSs are systems that realize intrusion detection logging the information detected and alerting predefined procedures.

They can be either hardware or software. As reported in the following list, mainly there are three types of IDS in Clouding.

- Host Based IDSs (HIDS): analyze the suspicious processes like threads, system call and configuration access by observing the situation of Host. They're usually used to protect server systems. HIDS are composed by sensors located on servers in order to prevent the attacks to a Host. HIDS can also monitor network traffic and it can also trace more and settle with local settings of an OS logging records;

- Network-based IDSs (NIDS): monitor and analyze the specified network traffic. They can detect different situations based on specified points and generally located between the end point devices like routers or firewalls. A NIDS attempts to discover unauthorized access to a network by analyzing traffic for signs of malicious activities and events. Network traffic works at different network layers and every layer delivers the data coming from a layer to another layer. OSI reference model define how these layers works and manages the traffic;

- Distributed IDS (DIDS): model of intrusion detection in a distributed environment such as Clouding. All the components communicate with each other with an agent-based approach. Main subject in DIDSs deal whole system like a traditional network or Host. DIDS components do not have a standard, but there are network and Host-based sensor components, detection engine and management component;

- Network Behavior Analysis IDS (NBAIDS): decide if the network traffic is suspect by mean of statistical data models of network traffic. Sensors detect DoS attacks with the help of to be aware of the network traffic and unexpected application services and rule violations by scanning the network. Normally NIDSs and NBAD systems share some sensor and management consoles, but NBAD systems generally do not have database servers. NBAD systems work to decide in the case of unexpected data traffic, they're used to detect worms and DoS attacks.

Intrusion Prevention Systems (IPS)

IPS holds all capabilities of IDSs adding some prevention capabilities. IPSs can change configurations of network devices: if an intrusion was detected a firewall rule will be applied changing either the routing configuration or a VM will be isolated among security procedures.

Because of the distributed nature of Clouding, all monitored and prevented resources are taken place in many different locations, they could be even in different countries. Thus, intrusion detection sensors placement, collecting intrusion data, analyzing by detection engines and interfering for prevention precautions are arduous task accomplish. At the same time: load balancing, resources allocation, bandwidth usage and so the whole price because of pay per usage model is the areas to be overcome.

Conclusion

This article starts describing the common type of Clouding service models.

Then, the article shows a list of yet open security issues belonging to Cloud model and mainly inherent to IaaS platforms, the problems reported also concern VoIP technologies hosted by Clouding. The threats are then specialized for the UC environment, where they must be adressed in a serious manner since if they was exploited by smart attackers, they could be harmful both for the user and Cloud providers. Finally the article reports the coutermeasures which should be adopted in order to protect a VoIP networks in a Cloud environment: IDS and IPS.

About the Author

Mirko Raimondi obtained his Master's degree in Computer Science from the University of Milan – Computer Science Department. He worked as a Software Engineer at ITALTEL – an Italian leader company in telecommunications industry – where he was being the project leader of Netmatch-S Lite Edition, a VoIP Session Border Controller based on virtual platform and running on commercial hardware. In test plant of ITALTEL he realized testing scenarios by mean of Cisco L2/L3 devices and he has a CCNA-security in course. Currently he works in automotive industry, where he has realized an audio/video/meta-data multiplexer in order to hide GPS data in mov files. He's interested in VoIP telecommunications, network security, steganography meth-ods and computer forensics. You can contact him either through LinkedIn: http://it.linkedin.com/pub/mirko-raimondi/14/182/58a or via e-mail: web.mirk@gmail.com.

UPDATE NOW WITH STIG AUDITING

"IN SOME CASES **nipper studio** HAS VIRTUALLY **REMOVED** the NEED FOR a **MANUAL AUDIT**"

CISCO SYSTEMS INC.

Titania's award winning Nipper Studio configuration auditing tool is helping security consultants and end-user organizations worldwide improve their network security. Its reports are more detailed than those typically produced by scanners, enabling you to maintain a higher level of vulnerability analysis in the intervals between penetration tests.

Now used in over 45 countries, Nipper Studio provides a thorough, fast & cost effective way to securely audit over 100 different types of network device. The NSA, FBI, DoD & U.S. Treasury already use it, so why not try it for free at www.titania.com

2012 Computing Security Awards WINNER Enterprise Security Solution of the Year

Security Products' GOVIES 2013 Government Security Awards

2012 Computing Security Awards WINNER Network Security Solution of the Year

www.titania.com

D.I.M.
DIGITAL INVESTIGATION MANAGER

The **only** existing System of its kind,
IncMan Suite has already been adopted
by a host of corporate clients worldwide

The Ultimate
Forensic Case Management Software

Fully automated Encase Integration

Evidence tracking and Chain of Custody

Supports over 50 Forensic Software and third parties

Training and Certification available

Special discount for LEO, GOV and EDU customers

DFLabs
Managing Infosecurity Risks

SPECIAL PROMO 15% OFF

single user perpetual license

http://www.dimmodule.com

promo code E-FORNCS13

DFLabs DIM is a forensic case management software that coherently manages cases, data input and modifications carried out by the different operators during Digital Evidence Tracking and Forensics Investigations.

It is part of the IncMan Suite, thus it is able to support the entire Computer Forensics and Incident Response workflow and compliant with the ISO 27037 Standard.

www.digitalinvestigationmanager.com